UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/661,696	09/12/2003	David D. Brandt	03AB014C/ALBRP303USC	7375

7590 04/05/2011

Susan M. Donahue
Rockwell Automation, 704-P, IP Department
1201 South 2nd Street
Milwaukee, WI 53204

EXAMINER	
BAUM, RONALD	

ART UNIT	PAPER NUMBER
2439	

MAIL DATE	DELIVERY MODE
04/05/2011	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/661,696
Filing Date: September 12, 2003
Appellant(s): BRANDT ET AL.

Brian Steed, Reg. No. 64,095
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 1/3/2011 appealing from the Office action mailed 8/2/2010.

(1) Real Party in Interest

The examiner has no comment on the statement, or lack of statement, identifying by name the real party in interest in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The examiner has no comment on the appellant's statement of the status of amendments after final rejection contained in the brief.

(5) Summary of Claimed Subject Matter

The examiner has no comment on the summary of claimed subject matter contained in the brief.

(6) Grounds of Rejection to be Reviewed on Appeal

The examiner has no comment on the appellant's statement of the grounds of rejection to be reviewed on appeal. Every ground of rejection set forth in the Office action from which the appeal is taken (as modified by any advisory actions) is being maintained by the examiner except for the grounds of rejection (if any) listed under the subheading "WITHDRAWN

REJECTIONS." New grounds of rejection (if any) are provided under the subheading "NEW GROUNDS OF REJECTION."

(7) Claims Appendix

The examiner has no comment on the copy of the appealed claims contained in the Appendix to the appellant's brief.

(8) Evidence Relied Upon

7,013,395 B1	Swiler et al	3-2006
6,374,358 B1	Townsend	4-2002
2004/0059920 A1	Godwind	3-2004

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-9, 12-17, 19-21, 23, 25, 30, 41 and 45-52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Swiler et al, U.S. Patent 7,013,395 B1 in view of Townsend, U.S. Patent 6,374,358 B1, and further in view of Godwind, U.S. Patent Publication US 2004/0059920 A1.

Prior Art's Broad Disclosure vs. Preferred Embodiments

As concerning the scope of applicability of cited references used in any art rejections below, as per MPEP § 2123, subsection R.5. Rejection Over Prior Art's Broad Disclosure Instead of Preferred Embodiments:

1. PATENTS ARE RELEVANT AS PRIOR ART FOR ALL THEY CONTAIN "The use of patents as references is not limited to what the patentees describe as their own inventions or to the problems with which they are concerned. They are part of the literature of the art, relevant for all they contain." In re Heck, 699 F.2d 1331, 1332-33, 216 USPQ 1038, 1039 (Fed. Cir. 1983) (quoting In re Lemelson, 397 F.2d 1006, 1009, 158 USPQ 275, 277 (CCPA 1968)). A reference may be relied upon for all that it would have reasonably suggested to one having ordinary skill the art, including nonpreferred embodiments. Merck & Co. v. Biocraft Laboratories, 874 F.2d 804, 10 USPQ2d 1843 (Fed. Cir.), cert. denied, 493 U.S. 975 (1989). See also > Upsher-Smith Labs. v. Pamlab, LLC, 412 F.3d 1319, 1323, 75 USPQ2d 1213, 1215 (Fed. Cir. 2005)(reference disclosing optional inclusion of a particular component teaches compositions that both do and do not contain that component);< Celeritas Technologies Ltd. v. Rockwell International Corp., 150 F.3d 1354, 1361, 47 USPQ2d 1516, 1522-23 (Fed. Cir. 1998) (The court held that the prior art anticipated the claims even though it taught away from the claimed invention.). >See also MPEP § 2131.05 and § 2145, subsection X.D., which discuss prior art that teaches away from the claimed invention in the context of anticipation and obviousness, respectively.<

II. NONPREFERRED AND ALTERNATIVE EMBODIMENTS CONSTITUTE PRIOR ART
Disclosed examples and preferred embodiments do not constitute a teaching away from a broader disclosure or nonpreferred embodiments. In re Susi, 440 F.2d 442, 169 USPQ 423 (CCPA 1971). "A known or obvious composition does not become patentable simply because it has been described as somewhat inferior to some other product for the same use." In re Gurley, 27 F.3d 551, 554, 31 USPQ2d 1130, 1132 (Fed. Cir. 1994). Furthermore, "[t]he prior art's mere disclosure of more than one alternative does not constitute a teaching away from any of these alternatives because such disclosure does not criticize, discredit, or otherwise discourage the solution claimed…." In re Fulton, 391 F.3d 1195, 1201, 73 USPQ2d 1141, 1146 (Fed. Cir. 2004).

Swiler et al generally teaches and suggests (i.e., Abstract, figures 1-2 and associated descriptions in general) the limitations set forth in the claims below (e.g., claim 1), as modified by the Townsend and Godwin teachings as further described below.

5. As per claim 1; "A security analysis tool for an automation system having a controller, an I/O device, and a controlled device, the I/O device being configured to at least one of provide output data to control the controlled device or receive input data from the controlled device, the controller being configured to at least one of provide the output data to the I/O device or receive the input data from the I/O device, the controller also having a memory configured to store the input data and output data in an I/O table, the memory further configured to store a control program that uses the I/O table to control the controlled device, the security analysis tool comprising:

a learning component that

monitors the communication of data

associated with the I/O table

during a training period and

generates a learned pattern of communication [figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology (i.e., description of **factory assets**, *inclusive of system information acquisition ('*... a learning component ... monitors the communication of data ... during a training period ') as part of the monitoring/scanning of communications to/from the network computer, whereas for the case of factory automation IT/network elements involved in the operation of a given commercial/industrial/government environment (e.g., col. 1,lines 24-45, col. 5,lines 30-55) encompasses the use of - at the very least - programmable logic controllers of which industrial controllers are an associated architecture), such that industrial controllers running standard operating systems (e.g., col. 2,lines 3-67; UNIX, Windows, etc.,) use I/O data structures to at least deal with interface processing (e.g., I/O tables involved in port communications (i.e., hardware driver support of serial ports, parallel ports, USB ports, and communications ports that deal with both a port physical network address and associated application involved during packet communications generally; '... I/O device ... I/O table *...') processing, etc.,), clearly de*aling with Intranet/Internet access patterns insofar as network security per se is concerned) and attack template (i.e., *a model; '*... generates a learned pattern of communication *...') information dealing with* hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.]; and

an analyzer component that

monitors data traffic

subsequent to the training period and

generates one or more security outputs

if a current pattern of the data traffic deviates

from the learned pattern

in excess of the acceptable deviation [figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology and attack template information, such that results (i.e., post analysis generated se*curity outputs; '...* generates one or more security outputs *...') used to evaluate (i.e., graphed output* information)/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended (relative to the learned/acquired model/template; ' ... from the learned pattern *...'), clearly encompassing the claimed* limitations as broadly interpreted by the examiner.],

the one or more security outputs including

at least one output that alters the data traffic between the controller and

the at least one I/O device [Townsend and further in view of Godwind below].

It is noted that Swiler et al, does not disclose the specific type of action taken upon vulnerability assessment results determination, insofar as additional security components are required (i.e., installation) upon a vulnerability or detected security problem so determined. However, the examiner asserts that it would have been obvious to one ordinary skill in the art at the time the invention was made for the adaptive countermeasure selection method/apparatus of Townsend to be combined with the validation component vulnerability assessment results of Swiler et al, insofar as the Swiler et al teaching of a computer system analysis tool **requiring a responding mechanism to make use of the analysis tool output** (i.e., the Townsend countermeasure selection method/apparatus installation countermeasures aspects, col. 3,lines 17-33, col. 7,lines 33-65), and would be in itself an obvious intended use. However, Townsend does not explicitly deal with the automated aspect of the countermeasures. Godwin teaches of using an automated tool to automatically (e.g., Godwin, ¶0019-0022, 0031) adjust security parameters (i.e., again, as a result of the Townsend countermeasure selection method/apparatus installation countermeasures aspects) for **online** storage systems (e.g., the industrial controller storage functionality per se in the industrial control/enterprise environment), encompassing communications control – broadly – insofar as access control to a network storage entity constitutes output control correction relative to a prior network communications state. Further, Godwind teaches the checking/editing/updating/etc., of security settings manually (e.g., Godwin,

¶0019-0022, 0031, 0073-0136, inclusive of bounds limitations on the parameter determination updating, etc.,) for network processing computers/processing elements, upon discerning via a security policy/rules criteria analysis that said security settings require said editing/updating/etc., is costly and error prone, and can be enhanced via automating the process.

Such motivation to combine would clearly be an obvious requirement, insofar as using the validation component vulnerability assessment results of Swiler et al to require the vulnerability results to be utilized as a practical business aspect of requiring the vulnerability assessment in the first place (e.g., Townsend business concerns requiring countermeasures, col. 3,lines 1-50), as implemented in an automated manor because of the costly and error prone checking/editing/updating/etc., of security settings manually for network processing computers/processing elements, upon discerning via a security policy/rules criteria analysis that said security settings require said editing/updating/etc.

A recitation directed to the manner in which a claimed apparatus is intended to be used does not distinguish the claimed apparatus from the prior art if prior art has the capability to do so (See MPEP 2114 and Ex Parte Masham, 2 USPQ2d 1647 (1987).

As per claim 12, this claim is the method claim for the system claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection.

As per claim 16, this claim is the means plus function claim for the system claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection.

As per claim 17, this claim is an apparatus (a security validation system) claim variation for the (security analysis tool) system claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection, insofar as the claim 1 tool results in effective security validation as a function of the security output aspects of the claims.

As per claim 30, this claim is the means plus function claim for the system claim 17 above, and is rejected for the same reasons provided for the claim 17 rejection.

6. Claim 2 **additionally recites** the limitation that; "The tool of claim 1, further comprising an interface component

that generates a description of

one or more industrial controllers in the automation system".

The teachings of Swiler et al are directed towards such limitations, as modified by Townsend in view of Godwind as discussed in claim 1 above (i.e., figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted (i.e., interface component) computer system/network configuration/topology (i.e., description of factory assets - clearly ' industrial controllers in the automation system ') and attack template (i.e., model; '... generates a description of ...') information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

7. Claim 3 **additionally recites** the limitation that; “The tool of claim 2, wherein at least one of the interface component or the analyzer component

operate on a computer and

receive one or more factory inputs that provide the description,

the factory inputs include at least one of

user input,

model inputs,

schemas,

formulas,

equations,

files,

maps, or

codes.”.

The teachings of Swiler et al are directed towards such limitations, as modified by Townsend in view of Godwind as discussed in claim 1 above (i.e., figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted (i.e., interface component utilizing, at the very least, user input, model inputs, files, maps, and codes) computer system/network configuration/topology (i.e., description of factory assets) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

8. Claim 4 **additionally recites** the limitation that; "The tool of claim 3, wherein

the factory inputs are processed by

the analyzer component to generate the security outputs,

the security outputs including

at least one of

manuals,

documents,

schemas,

executables,

codes,

files,

e-mails,

recommendations,

topologies,

configurations,

application procedures,

parameters,

policies,

rules,

user procedures, or

user practices

that are employed

to facilitate security measures in

an automation system.".

The teachings of Swiler et al are directed towards such limitations, as modified by Townsend in view of Godwind as discussed in claim 1 above (i.e., figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology and attack template information, such that results (i.e., post analysis generated security outputs) used to evaluate (i.e., graphed output information, utilizing, at the very least, topologies, recommendations, files, rules, configurations)/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

9. Claim 5 **additionally recites** the limitation that; "The tool of claim 2, wherein

the interface component includes

at least one of

a display output having associated display objects and

at least one input

to facilitate operations with

the analyzer component,

the interface component is associated with

at least one of

an engine,

an application,

an editor tool,

a web browser, or

a web service.".

The teachings of Swiler et al are directed towards such limitations, as modified by Townsend in view of Godwind as discussed in claim 1 above (i.e., figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted (i.e., interface component, utilizing, at the very least, input editing tools, and a display output having associated display objects for the results graphic output) computer system/network configuration/topology (i.e., description of factory assets) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

10. Claim 6 **additionally recites** the limitation that; "The tool of claim 5, wherein

the display objects include

at least one of

configurable icons,

buttons,

sliders,

input boxes,

selection options,

menus, or

tabs,

the display objects having

multiple configurable

dimensions,

shapes,

colors,

text,

data and

sounds

to facilitate operations with

the analyzer component.".

The teachings of Swiler et al are directed towards such limitations, as modified by Townsend in view of Godwind as discussed in claim 1 above (i.e., figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted (i.e., interface component, utilizing, at the very least, GUI oriented input editing tools, and a display output having associated display objects for the results graphic output) computer system/network configuration/topology (i.e., description of factory assets) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

11. Claim 7 **additionally recites** the limitation that; "The tool of claim 5,

the at least one input includes

user commands from at least one of

a mouse,

a keyboard,

speech input,

a web site,

a remote web service,

a camera, or

video input

to affect operations of

the interface component and

the analyzer component.".

The teachings of Swiler et al are directed towards such limitations, as modified by Townsend in view of Godwind as discussed in claim 1 above (i.e., figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted (i.e., interface component, utilizing, at the very least, GUI oriented input editing tools, and a display output having associated display objects for the results graphic output) computer system/network configuration/topology (i.e., description of factory assets) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

12. Claim 8 **additionally recites** the limitation that; "The tool of claim 2, wherein

the description includes

a model of one or more industrial automation assets

to be protected and

associated network pathways

to access the one or more industrial automation assets.".

The teachings of Swiler et al are directed towards such limitations, as modified by Townsend in view of Godwind as discussed in claim 1 above (i.e., figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology (i.e., description of **factory assets** whereas factory automation IT/network elements involved in the operation of a given commercial/industrial/government environment (e.g., col. 1,lines 24-45, col. 5,lines 30-55) encompasses the use of at the very least programmable logic controllers of which industrial controllers are an associated architecture) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

13. Claim 9 **additionally recites** the limitation that; "The tool of claim 2, wherein

the description

includes at least one of

risk data or

cost data

that is employed by

the analyzer component

to determine suitable security measures.".

The teachings of Swiler et al are directed towards such limitations, as modified by Townsend in view of Godwind as discussed in claim 1 above (i.e., figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology (i.e., description of factory assets) and attack template (i.e., model, clearly dealing with risk and effective cost insofar as network security per se is concerned) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

As per claim 13, this claim is the method claim for the system claim 9 above, and is rejected for the same reasons provided for the claim 9 rejection.

14. Claim 14 **additionally recites** the limitation that; "The method of claim 13, wherein generating the one or more security outputs includes

generating one or more security outputs that include

at least one of recommended

security components,

codes,

parameters,

settings,

related interconnection topologies,

connection configurations,

application procedures,

security policies,

rules,

user procedures, or

user practices.".

The teachings of Swiler et al are directed towards such limitations, as modified by Townsend in view of Godwind as discussed in claim 1 above (i.e., figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology and attack template information, such that results (i.e., post analysis generated security outputs) used to evaluate (i.e., graphed output information, utilizing, at the very least, topologies, recommendations, files, rules, configurations)/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

15. Claim 15 **additionally recites** the limitation that; "The method of claim 13, further comprising:

automatically deploying the one or more security outputs

to the industrial controller; and

utilizing the security outputs

to mitigate at least one of

unauthorized network access and

network attack.".

The teachings of Swiler et al are directed towards such limitations, as modified by Townsend in view of Godwind as discussed in claim 1 above (i.e., figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology and attack template information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

16. Claim 19 **additionally** recites the limitation that; "The system of claim 17, further comprising:

a scanner component that automatically interrogates

at least one of

the industrial controller,

the I/O device, or

the controlled device

at periodic intervals for security-related data [figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology (i.e., polling/automatically interrogating of network machines (periodic interval scanning) and gathering associated data such as IP address, machine type, operating system, file system structure, etc.,) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.];

a validation component that automatically assesses security capabilities

of the at least one of

the industrial controller,

the I/O device, or

the controlled device

based upon a comparison of

the security-related data and

one or more predetermined security guidelines [figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology (i.e., polling/automatically interrogating of network machines (periodic interval scanning) and gathering associated data such as IP address, machine type, operating system, file system structure, etc.,) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities *(i.e., a validation component ...) as a function of the risks and costs associated* with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.]; and

a security analysis tool that recommends

at least one network interconnection

to achieve a specified security goal [figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology and attack template information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes (i.e., ' security analysis tool ... recommends interconnection ... a specified security goal ') in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.]

indicated by the predetermined security guidelines.".

The teachings of Swiler et al are directed towards such limitations, as modified by Townsend in view of Godwind as discussed in claim 1 above.

17. Claim 20 **additionally recites** the limitation that; "The system of claim 19, wherein

the security guidelines

are automatically determined.".

The teachings of Swiler et al are directed towards such limitations, as modified by Townsend in view of Godwind as discussed in claim 1 above (i.e., figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology and attack template information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

18. Claim 21 **additionally recites** the limitation that; "The system of claim 46, wherein

the host-based component performs

vulnerability scanning and

auditing on devices, and

the network-based component performs

vulnerability scanning and

auditing on networks.".

The teachings of Swiler et al are directed towards such limitations, as modified by Townsend in view of Godwind as discussed in claim 1 above (i.e., figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system (i.e., host-based/network-based component) analysis tool using inputted (i.e., vulnerability scanner component) computer system/network configuration/topology (i.e., auditing factory assets) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended (i.e., validation component), clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

19. Claim 23 **additionally recites** the limitation that; "The system of claim 21, wherein

at least one of

the host-based component or

the network-based component

at least one of

non-destructively maps a topology of

information technology (IT) and

industrial automation devices,

checks revisions and configurations,

checks user attributes, or

checks access control lists.".

The teachings of Swiler et al are directed towards such limitations, as modified by Townsend in view of Godwind as discussed in claim 1 above (i.e., figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system (i.e., host-based/network-based component) analysis tool using inputted (i.e., vulnerability scanner component) computer system/network configuration/topology (i.e., auditing of **factory assets** whereas factory automation IT/network elements involved in the operation of a given commercial/industrial/government environment (e.g., col. 1,lines 24-45, col. 5,lines 30-55) encompasses the use of at the very least programmable logic controllers of which industrial controllers are an associated architecture) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended (i.e., validation component), clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

20. Claim 25 **additionally recites** the limitation that; "The system of claim 17, wherein the security action includes at least one of

automatically correcting the security events,

automatically adjusting security parameters,

altering network traffic patterns,

adding security components,

removing security components,

triggering alarms,

automatically notifying entities about detected problems and concerns,

generating an error or log file,

generating a schema,

generating data to re-configure or re-route network connections,

updating a database, or

updating a remote site.

The teachings of Swiler et al are directed towards such limitations, as modified by Townsend in view of Godwind as discussed in claim 1 above (i.e., figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology and attack template information, such that results (i.e., post analysis generated security outputs) used to evaluate (i.e., graphed output information, utilizing, at the very least, topologies, recommendations, files, rules, configurations)/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, such that as modified by the Townsend in view of Godwind teachings to an applied network configuration, deal with the actual use of the combination (i.e., the security action per se encompassing the various limitations of this claim; '… automatically correcting the security events … removing security components … generating data to re-configure or re-route network connections …'), clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

21. Claim 45 **additionally recites** the limitation that; "The tool of claim 1,

the analyzer component is adapted for

partitioned security specification entry and

sign-off from various groups.".

The teachings of Swiler et al are directed towards such limitations, as modified by Townsend in view of Godwind as discussed in claim 1 above (i.e., figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology (i.e., the network partitioned security specification) and attack template (i.e., inclusive of authentication aspects, insofar as sign-on/sign-off, at the very least would be concerned) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

22. Claim 46 **additionally recites** the limitation that; "The system of claim 19,

the scanner component and

the validation component

are at least one of

a host-based component or

a network-based component.".

The teachings of Swiler et al are directed towards such limitations, as modified by Townsend in view of Godwind as discussed in claim 1 above (i.e., figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system (i.e., host-based/network-based component) analysis tool using inputted (i.e., scanner component) computer system/network configuration/topology (i.e., description of factory assets) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended (i.e., validation component), clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

23. Claim 47 **additionally recites** the limitation that; "The system of claim 21,

at least one of

the host-based component or

the network-based component

at least one of

determines susceptibility to

common network-based attacks,

searches for

open Transmission Control Protocol/User Datagram Protocol (TCP/UDP)

ports,

scans for

vulnerable network services,

attempts to gain identity information about

end devices that relates to

hacker entry, or

performs vulnerability

scanning and

auditing

on

firewalls,

routers,

security devices, and

factory protocols.".

The teachings of Swiler et al are directed towards such limitations, as modified by Townsend in view of Godwind as discussed in claim 1 above (i.e., figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system (i.e., host-based/network-based component) analysis tool using inputted (i.e., vulnerability scanner component) computer system/network configuration/topology (i.e., auditing factory assets) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended (i.e., validation component), clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

24. Claim 48 **additionally** recites the limitation that; "The system of claim 41, the validation component automatically installs

one or more security components

in response to the one or more vulnerabilities.".

The teachings of Swiler et al are directed towards such limitations, as modified by Townsend in view of Godwind as discussed in claim 1 above (i.e., figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology and attack template information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended (i.e., validation component, insofar as associated with improper configuration, vulnerability, file system check, user privileges check, etc.,), as modified by Townsend/Godwin insofar as the automated update of security parameters corresponds to said parameters as part of the installation criteria of the security parameters/components for the industrial controller environment, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

25. Claim 49 **additionally** recites the limitation that; "The system of claim 1, wherein the analyzer component further

performs an automated action that disables network requests

from at least one outside network

upon detecting that

the current pattern of the data traffic deviates

from the learned pattern

in excess of the acceptable deviation.".

The teachings of Swiler et al are directed towards such limitations, as modified by Townsend in view of Godwind as discussed in claim 1 above (i.e., figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology and attack template information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended (i.e., validation component, insofar as associated with improper configuration, vulnerability, file system check, user privileges check, etc.,), as modified by Townsend/Godwin insofar as the automated update of security parameters ('… disables network requests … upon detecting … current pattern of the data traffic deviate …') corresponds to said parameters as part of the installation criteria ('… in excess of a threshold …' e.g., Godwin, ¶0071-0078) of the security parameters/components for the industrial controller environment, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

26. Claim 50 **additionally** recites the limitation that; "The system of claim 12, wherein the at least one automated security event includes

at least disabling network attempts to access the industrial controller.".

The teachings of Swiler et al are directed towards such limitations, as modified by Townsend in view of Godwind as discussed in claim 1 above (i.e., figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology and attack template information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended (i.e., validation component, insofar as associated with improper configuration, vulnerability, file system check, user privileges check, etc.,), as modified by Townsend/Godwin insofar as the automated update of security parameters/events corresponds to said parameters/events as part of the installation criteria of the security parameters/events/components for the industrial controller environment, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

27. Claim 51 **additionally** recites the limitation that; "The method of claim 12, wherein the monitoring communication of data comprises at least one of

monitoring a number of network requests

to or from the industrial controller

over a given time frame or

monitoring a type of request

to or from the industrial controller

during the training period.

The teachings of Swiler et al are directed towards such limitations, as modified by Townsend in view of Godwind as discussed in claim 1 above (i.e., figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted (i.e., vulnerability scanner component, inclusive of monitored/scanned information comprising the packet information, that upon being stored/logged ('... monitoring a number of network requests ...') is such that stored log lines/events represent time tagged events ('... over a given time frame ...') that are descriptive of the communications event (i.e., port number; '... monitoring a type of request ...') per se) computer system/network configuration/topology/attack template information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

28. Claim 52 **additionally** recites the limitation that; “The tool of claim 1, wherein the one or more security outputs alter the data traffic between

the controller and

the at least one I/O device to restore the learned pattern.

The teachings of Swiler et al are directed towards such limitations, as modified by Townsend in view of Godwind as discussed in claim 1 above (i.e., figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology and attack template information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities (as a function of the risks and costs associated with the changes recommended), as modified by Townsend/Godwin insofar as the automated update of security parameters subsequently applied to remediation of the determined vulnerability ('… security outputs … alter the data traffic between … controller …') for the industrial controller networked ('… at least one I/O device to restore the learned pattern …') environment, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

(10) Response to Argument

A-1) In response to the appellant's arguments regarding independent claims 1, 12, 16, 17 and 30 (and claims 2-9, 13-15, 19-21, 23, 25, 41 and 45-52 by dependency), the appellant argues that the references of Swiler et al, Townsend and/or Godwin do not disclose or suggest “a learning component that monitors the communication of data associated with the I/O table during a training period and generates a learned pattern of communication”. The Examiner respectfully disagrees, the Examiner uses the reference Swiler et al to teach, at least, the “a learning component that monitors the communication of data associated with the I/O table during a training period and generates a learned pattern of communication” claim aspect, insofar as the reference of Swiler et al discloses in, at least, figures 1-2 and associated descriptions, and more succinctly col. 1,lines 16-23, col. 4,lines 33-58**,** and col. 5,lines 55-col. 6,line 2, the aspects of: (1) “a learning *component*…” that is embodied in the modeling of network risks via an attack graph (e.g., col. 4,lines 33-42) that is a function of at least the attack templates and attacker profiles – both learned parameters used in the attack graph generation – that are combined with (i.e., in the context of) the configuration file (e.g., col. 4,lines 43-58), where the configuration file is a function of network topology detailed configurations of particular elements (e.g., col. 5,lines 55-col. 6,line 2; IP addresses, port numbers/associated services), clearly "[a] **learning** component **that monitors** the **communication** ... during a **training period** and **generates** a learned **pattern of communication**", given that the particular elements information had to have been monitored to be gathered to make the configuration file, and (2) "... **communication** of **data associated with the I/O table**..." that is embodied in the (col. 5,lines 55-col. 6,line 2) IP addresses, port numbers/associated services, etc., aspects of the configuration file – insofar as IP addresses, port number/services are clearly embodied as table based data structures per se.

Further, as per the Appellant's representative interpretation of the Swiler et al "architectural information" regarding the system being analyzed not being equivalent to the claimed "... component that **monitors the communication of data** ...", the examiner – using the broadest reasonable interpretation – disagrees, insofar as the "architectural information" that consists of system acquired (i.e., learned via a monitoring of the information) IP addresses, port number/services that are the parameters gathered in any monitoring of communications of "... data associated with ... during a ... period ..." (e.g., a log/log file, cache, buffer, or whatever data structure used to store captured monitored network information).

Still further, as per the Appellant's representative interpretation of the Swiler et al "network configuration/topology information provided to the cited analysis tool via the configuration file" not reading on the claimed "... component that **monitors the communication of data** ..." using an analysis tool per se, the examiner – using the broadest reasonable interpretation – disagrees, insofar as the various descriptions of the elements and method associated with the Swiler et al implementation(s) of the data gathering throughout the attack template, profile, configuration (e.g., col. 1,lines 16-23, col. 5,lines 55-col. 6,line 2) and subsequent use in the analysis and associated reporting/rendering, etc., of the analysis result(s), clearly encompasses an analysis tool use, insofar as the claim language does not explicitly patently distinguish the analysis tool beyond a general description.

Still further, as per the Appellant's representative interpretation of the Townsend and/or Godwin references to cure the alleged deficiencies in the claims concerning the above described claim limitation aspect dealing with *"a* learning component that monitors the *communication ...* during a training period and generates a learned pattern of communication*"*, the examiner disagrees, insofar as the Townsend and/or Godwin references are used as a rejection of the subsequent security outputs and actions taken claim limitation aspects (see **A-2** below), and not the *"a* learning component ... *monitors the communication ... training period ...* learned pattern of communication*"* limitation(s).

A-2) In response to the appellant's arguments regarding independent claims 1, 12, 16, 17 and 30 (and claims 2-9, 13-15, 19-21, 23, 25, 41 and 45-52 by dependency), the appellant argues that the references of Swiler et al, Townsend and/or Godwin do not disclose or suggest "an analyzer component that monitors data traffic subsequent to the training period and generates one or more security outputs if a current pattern of the data traffic deviates from the learned pattern in excess of the acceptable deviation". The Examiner respectfully disagrees, the Examiner uses the reference Swiler et al to teach, at least (see **A-1** above), the "a learning component that monitors the communication of data associated with the I/O table during a training period and generates a learned pattern of communication" claim aspect, such that the subsequent use of "[an] analyzer component that monitors data traffic subsequent to the training period and generates one or more security outputs if a current pattern of the data traffic deviates from the learned pattern in excess of the acceptable deviation" is the Townsend and/or Godwin references teachings aspect of the 35 U.S.C. 103(a) rejection modification to the teachings of Swiler et al, insofar as teaching the obvious security outputs and actions taken aspects (e.g., Swiler et al, col. 8,lines 6-37) of the claim is concerned.

More succinctly, the adaptive countermeasure selection method/apparatus of Townsend combined with the validation component vulnerability assessment results of Swiler et al, insofar as the Swiler et al teaching of a computer system analysis tool **requiring a responding mechanism to make use of the analysis tool output** (i.e., the Townsend countermeasure selection method/apparatus installation countermeasures aspects, col. 3,lines 17-33, col. 7,lines 33-65), would be in itself an obvious intended use "[of an] analyzer component that monitors ... subsequent to ... training ... and generates one or more security outputs if ... traffic deviates from ... learned pattern ...". Godwin teaches of using an automated tool to automatically (e.g., Godwin, ¶0019-0022, 0031) adjust security parameters (i.e., again, as a result of the Townsend countermeasure selection method/apparatus installation countermeasures aspects) for **online** storage systems (e.g., the industrial controller storage functionality per se in the industrial control/enterprise environment), encompassing communications control – broadly – insofar as access control to a network storage entity constitutes output control correction relative to a prior network communications state. Further, Godwind teaches the checking/editing/updating/etc., of security settings manually (e.g., Godwin, ¶0019-0022, 0031, 0073-0136, inclusive of bounds limitations on the parameter determination updating, etc.,) for network processing computers/processing elements, upon discerning via a security policy/rules criteria analysis that said security settings require said editing/updating/etc., is costly and error prone, and can be enhanced via automating the process.

Further, as per the Appellant's representative interpretation of the Townsend and/or Godwin references not curing the alleged deficiencies in the claims concerning "[an] analyzer component ... generates one or more security **outputs if** ... **traffic deviates** from ... learned pattern ...", the examiner disagrees, insofar as the Townsend and/or Godwin references – as described above – are clearly concerned with the results and automated aspects of dealing with determined results of the analysis.

A-3) In response to the appellant's arguments regarding dependent claim 49, the appellant argues that the references of Swiler et al, Townsend and/or Godwin do not disclose or suggest "the analyzer component further performs an automated action that disables network requests from at least one outside network upon detecting that the current pattern of the data traffic deviates from the learned pattern in excess of the acceptable deviation". The Examiner respectfully disagrees, insofar as Swiler et al teaching, at least (see **A-1** above), the "a learning component that monitors the communication of data associated with the I/O table during a training period and generates a learned pattern of communication" claim aspect; and the subsequent use of "[an] analyzer component that monitors data traffic subsequent to the training period and generates one or more security outputs if a current pattern of the data traffic deviates from the learned pattern in excess of the acceptable deviation" as taught by Townsend and/or Godwin references teachings aspect of the 35 U.S.C. 103(a) rejection modification to the teachings of Swiler et al (see **A-2** above), teaching of the obvious automated security outputs and actions taken aspects of the claim clearly encompasses the learning/analysis/automated output per se.

Further, as per the Appellant's representative interpretation of the Townsend and/or Godwin references not curing the alleged deficiencies in the claims concerning "... automated action that **disables network requests** ... outside network upon detecting ... current pattern of the data traffic deviates from the learned pattern in excess of the acceptable deviation", the examiner disagrees, insofar as the Townsend and/or Godwin references – as described above – are clearly concerned with the results and automated aspects of dealing with determined results of the analysis, of which the outputs that are used to modify the Swiler et al configuration file (e.g., col. 8,lines 6-37), clearly are subsequently reflected back at the output of the system, changing the configuration for the communications (e.g., figure 1, blocking input, as per a gateway/firewall function via port number, IP address filtering, etc., effectively "[an]... automated action that **disables network requests** ... **outside network** upon detecting ... current pattern of the data traffic deviates from the learned pattern in excess of the acceptable deviation").

(11) Information Disclosure

The information disclosure statement (IDS) submitted on 3/21/2011 was filed after the mailing date of the Final Office Action on 6/4/2010. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

(12) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/R. B./

Examiner, Art Unit 2439

Conferees:

/Edan Orgad/

Supervisory Patent Examiner, Art Unit 2439

/Christian LaForgia/
Primary Examiner, Art Unit 2439